WHAT IS CLAIMED IS:

1. A method of performing graded authentication of a user wherein the method obtains and evaluates circumstantial data associated with an authentication attempt, the method comprising:

obtaining user data from a user during an authentication attempt;

obtaining circumstantial data associated with the authentication attempt; and

determining a level of trust associated with the authentication attempt based on the comparison of the circumstantial data with previously stored data.

2. A method as in Claim 1 wherein said act of determining the level of trust associated with the authentication attempt is further based on the comparison of the user data with previously stored data.

3. A method as in Claim 1 wherein the previously stored data comprises in part a historical record of the circumstantial data obtained during previous successful authentications for the user.

4. A method as in Claim 1 wherein the circumstantial data comprises an identification associated with the system from which the user data is obtained.

5. A method as in Claim 4 wherein the identification comprises a processor serial number.

6. A method as in Claim 1 wherein the circumstantial data comprises an identification associated with the network location of the system from which the user data is obtained.

7. A method as in Claim 6 wherein the identification comprises an IP address.

8. A method as in Claim 1 wherein the circumstantial data comprises a time stamp associated with the time at which the user data was obtained.

9. A method as in Claim 1 wherein the circumstantial data comprises an identifier representing the medium over which the user data is obtained.

10. A method as in Claim 1 wherein the circumstantial data represents more than one circumstantial aspect of the authentication attempt.

11. A method as in Claim 10 wherein the circumstantial data comprises a time stamp associated with the time at which the user data was obtained and an identification associated with the network location of the system from which the user data is obtained.

12. A system for graded authentication comprising user data obtained from a user during at least one previously successful authentication attempt, circumstantial data associated with the at least one previously successful authentication attempt, and a trust engine which generates a level of trust associated with a current authentication attempt based on the comparison of circumstantial data associated with the current authentication attempt with the circumstantial data associated with the at least one previously successful authentication attempt.

13. A system as in Claim 12 wherein the user data represents an intent to assent to a transaction.

14. A system as in Claim 12 wherein the circumstantial data represents a network address associated with the authentication attempt.

15. A system as in Claim 12 wherein the circumstantial data represents a time stamp associated with the authentication attempt.

16. A system as in Claim 12 wherein the level of trust is also based upon the comparison of the user data to previously stored user data.

17. A method for authenticating a user comprising:
obtaining user data associated with an authentication operation;
obtaining metadata related to the authentication operation;
comparing the metadata with previously stored data; and
determining a level of trust associated with the authentication operation.

18. A method as in Claim 17 wherein the user data associated with the authentication operation represents the intent of a user to assent to a transaction.

19. A method as in Claim 18 wherein the metadata related to the authentication operation are made available at a later time to contest a repudiation of the authentication operation by the user.

20. A method as in Claim 17 wherein the act of determining a level of trust associated with the authentication operation comprises assigning a percentage to the authentication operation which represents the degree of confidence in the authentication of the user.

21. A method as in Claim 17 further comprising determining an intermediate level of trust associated with the metadata based upon the comparison of the metadata with previously stored data.

22. A method as in Claim 21 wherein the act of determining an intermediate level of trust comprises assigning a percentage to the metadata which represents the degree of correspondence between the metadata and the previously stored data.

23. A method as in Claim 22 wherein the act of determining a level of trust associated with the authentication operation comprises multiplying the percentage

representing the intermediate level of trust and a percentage which represents a degree of correspondence between the user data and the previously stored data.

24. A method as in Claim 23 wherein additional factors are used to weight the percentage representing the intermediate level of trust and the percentage which represents the degree of correspondence between the user data and the previously stored data differently.

~~25.~~ A method for authenticating a user comprising:

obtaining user data associated with an authentication operation;

obtaining metadata related to the authentication operation; and

determining a level of trust associated with the authentication operation based on the metadata.

26. A method as in Claim 25 wherein the act of determining a level of trust compares the metadata with previously stored data.

27. A method as in Claim 25 further comprising providing the user with a plurality of authentication techniques which may be used to generate the user data.

28. A method as in Claim 27 wherein the user data is generated using more than one of the plurality of authentication techniques.

29. A method as in Claim 28 wherein the user data generated using each authentication technique is compared with a different portion of a set of previously stored data.

~~30.~~ A method for grading an authentication operation that relies on a variable set of authentication techniques to obtain authentication data, the method comprising:

defining the reliability of a set of authentication techniques that may be used in an authentication operation;

receiving authentication data during an authentication operation, said authentication data generated using a subset of the authentication techniques;

determining the acceptability of the authentication data generated by each of the subset of authentication techniques; and

defining the level of trust of the authentication operation based upon the acceptability of the authentication data and based upon the reliability of the authentication techniques used in generating the authentication data.

31. The method of Claim 30 wherein the act of determining the acceptability involves comparing the authentication data with previously stored enrollment data.

32. The method of Claim 31 wherein the act of defining the reliability of a set of authentication techniques is based upon a set of circumstances associated with the previously stored enrollment data.

33. The method of Claim 30 wherein the act of defining the reliability of a set of authentication techniques is based upon the circumstances associated with the generation of the authentication data.

~~34.~~ An apparatus for evaluating an authentication attempt comprising:

reliability data associated with a set of authentication techniques that may be used in an authentication attempt;

a plurality of authentication instances generated using a subset of the authentication techniques; and

a trust engine which determines a level of match associated with each authentication instance and assigns a level of trust for the authentication attempt based upon the level of match associated with each authentication instance and the reliability of the technique used in each authentication instance.

35. An apparatus as in Claim 34 further comprising a required level of trust associated with the authentication attempt.

36. An apparatus as in Claim 35 wherein the trust engine further assigns a result for the authentication based upon a comparison of the level of trust associated with the authentication attempt and the required level of trust.

37. An apparatus as in Claim 35 wherein the required level of trust is determined by the trust engine based upon the risk associated with a successful authentication.

38. A method for grading an authentication attempt comprising:

defining the reliability of a set of authentication techniques that may be used in an authentication attempt;

receiving a plurality of authentication instances generated using a subset of the authentication techniques;

determining a level of match associated with each authentication instance; and

defining a level of trust of the authentication attempt based upon the level of match associated with each authentication instance and based upon the reliability of the technique used in each authentication instance.

39. A method as in Claim 38 further comprising defining a required level of trust for the authentication attempt.

40. A method as in Claim 39 further comprising assigning an authentication result to the authentication attempt based on a comparison of the level of trust for the authentication attempt and a required level of trust of the authentication attempt.

41. A method as in Claim 39 wherein the required level of trust for the authentication attempt is based upon the value associated with a successful authentication.

42. A method as in Claim 39 wherein the required level of trust for the authentication attempt is based upon the risk associated with a successful authentication.